INFORMATION WARFARE - Developing a Conceptual Framework

Top - Help

Draft 2.0 for Discussion Only

by LT (N) R Garigue - Strategic Information Technology Specialist
Office of the Assistant Deputy Minister (Defense Information Services)
garigue@dgs.drenet.dnd.ca - Url:http://www.cse.dnd.ca/~formis/overview/iw

In the course of reviewing and revising this document a special note of thank you for the contributions and comments by: Donna G. Schutzius, Major, USAF, Milan Kushta, Communication Security Establishment, DND, Tiit Rommet, Directorate Scientific and Technical Intelligence, DND, LeRoy Pearce, Senior Technology Advisor to ADM (DIS) DND

Thema

These rules, the sign language and grammar of the Game, constitute a kind of highly developed secret language drawing upon several science and arts, but especially mathematics and music, and capable of expressing and establishing interrelationships between the contents and the conclusions of nearly all scholarly disciplines, The Glass Bead Game is thus a mode of playing with the total contents and values of our culture; it plays with them as, say, in the great age of the arts painter might have played with the colors of his palette. All the insights, noble thoughts, and works of art that the human race has produced in its creative eras, all that subsequent periods of scholarly study have reduced to concepts and converted to intellectual property - on all this immense body of intellectual values the Glass Bead Game player plays like an organist on the organ.

```
            Herman Hess
Magister Ludi - The Glass Bead Game
    Translated from the German
        Das Glasperlenspiel
               1943
```

1. Introduction

Information has been recognized as a strategic resource which must be effectively managed to maintain a competitive and evolutionary advantage. Because of its critical role in reducing uncertainty, structuring complexity, and generating greater situational awareness, any action taken in the information domain can leverage tremendous effects in the physical domains of resources such as material, personnel and finance as well as more abstract domains such as belief systems. It also extend the range of new options for a planner or decision maker. As information is becoming more and more available in a digital format, ever increasingly powerful computational processes permits completely new forms of military endeavors that will require new organizations, activities, skills and mandates.

This essay introduces the concept of Information Warfare. It describes events in the development of computer technology which has lead to the development of the concept, describes and proposes a conceptual analysis framework to assist in the elopement of military new capabilities which will be required to respond to possible emerging vulnerabilities and opportunities.

The concept of Information Warfare (IW) may be considered as an overarching view of how modern warfare must be approached. It is a conceptual framework which assists in the development of not just military plans, projects, and capabilities, but how all government agencies involved in crisis management and conflict resolution. It also helps in the design, development and implementation of Command and Control Information Systems (C2IS).

With any new integrative concept, the notion of the paradigm arises. If the concept is sufficiently broad, then the new paradigm reveals both the flaws in the old way of thinking and offers at the same time new levels of efficiency and effectiveness enabled by new types of integrative processes. Information Warfare has been brought about by the Information Technology revolution, advances in Information Management (IM) and the emerging concerns for Knowledge Management. The Senior Technology Advisor to the Assistant Deputy Minister proposal on Information Management Core Capability Areas describes Information Warfare as one of the four central pillars supporting the Department of National Defense and the Canadian Forces vision of how to achieve Information Superiority in military affairs.

These for core capabilities are seen in fig 1 and are comprise of Joint Surveillance Systems, Information Technology, Knowledge Management for Decision Support and Information Warfare.

Figure 1
Core Capabilities

As will be shown in much more detail later Information Warfare includes military functions such as Information Collection Management, Assessment, Risk Assessment and Command and Control Warfare. But IW integrates these activities in a different and novel way through the use of modern information technologies. In many respect this is still uncharted territory for the military. Because of increased efficiency and effectiveness, Information Warfare has also some new inherent and totally distinct capabilities that emerge from this integration and the new "Domain" in which it occurs. Some call this "Domain": Cyberspace, others the National Information Infrastructure. Its name is less important than the fact that this new soci-technical space permits qualitatively superior levels of military and governmental action.

A note of prudence. In writing this document none of the functions were viewed with organizational structure in mind however in trying to describe some of the activities, references to present organizational structures are made. This is because sometimes new realities can only be described in terms of what is know and because of this analogical vice of discourse, some ambiguity and confusion remains. The development of a conceptual framework will help highlight what activities are truly new and what military activities are simply a recasting of know activities within this new Information Warfare framework.

More and more, the ability of the military to participate in employment that ranges across the full spectrum of conflict is dependent upon it's information processing capabilities, knowledge management and information system infrastructure. The ability to develop synergy and maintain network operations in the face of opposing disruptions is becoming the fundamental key to successful military action.

It is important to acknowledge that there is a wide and growing debate about what is Information Warfare. Several military structures are attempting to describe, agree and leverage the concept of Information Warfare. Some of these efforts are done without the benefit of having a consensus and agreement of what is Information Warfare. Some nations military have set up several Information Warfare units. In the US the Army, Navy and Air Force are trying to develop Information Warfare capabilities. The same debate is seen taking place in the UK and Australia.

Canada has just joined the Information Warfare discussions but has, at present, no organization that deals formally with the Information Warfare issues and concerns. One of the secondary objectives of this essay is to act as a means to raise the awareness on Information Warfare issues and help in planning any implementation.

2. Initial Conditions for the Emergence of Information Warfare

It is not possible to talk about Information Warfare without a brief discussion of the conditions which brought about its emergence. These conditions arise from the change in computer technology with its resulting impact on organization and decision making processes. The economics of computer production account for the lowering of cost and increased power account for the rapid spread of computer technology. In no other technical area is the cost of the required basic building block decreasing while at the same time increasing in performance in such a dramatic way. Many of the advances are being driven by the commercial needs of world wide market competition. The results of these developments can be brought to bear on Defense and Governmental efforts and activities as they pertain to conflict resolution, crisis management and military activities.

Some aspects of military information technology, however, will not be feasible without some DND R&D support and participation. Specifically long range communication, operation in harsh and hostile environments, identification of friend from foe, global positioning, imagery and visualization, network security, data and information fusion, and unique decision support tools and systems. These areas need to be further developed by DND if we want to be able to maintain world wide near real time awareness and participation in the full range of conflict resolution activities.

2.1 The Evolution of Computer Control

The computer has been in existence for more than 40 years. It has gone through four major architectural transformations. The type of control that they exercise upon processes have taken several forms. Each being more complex that the other. There has been a diffusion of control as the system have evolved. From a unique centrally control monolithic approach to a more democratic “peer to peer” collegiate type of control. Computers architecture have gone through the "Batch Processing" architecture, the "Time Sharing", the "The Desk Top" and now finally to the "Network" phase. This latest model will dominate and subsume all the others as the most efficient structure for controlling information processing. Naturally there will be further innovations as networks become pervasive and ubiquitous but the network model will be the one that will dominate the computing paradigm for years to come. Changes will have more to do with quantitative improvements rather than in the development of a radically new type of control structure. Intelligent and cooperative information systems using software agents are seen as the way to resolve the present problems of localized data dictionary and information model incompatibility. These harmonization efforts are focused on achieving "semantic interoperability". But this issue has more to do with ensuring common interpretation of the data -

the “meaning” problem- that the structural one on which network control is firmly established. The spread of the networks is an indication of its success.

2.2 The move from control to coordination

The development of the network also results in significantly different structure and pattern of problem solving work. Computer information networks break down strict hierarchies structures and organizational boundaries. It helps create virtual and distributed organizations focused more on the design and delivery of value added products and services. Mostly because “process” activities are taken care of by the computer information infrastructure and the network itself. Virtual workgroups concentrate their effort on the earlier phases of planning and problem solving The work they do may or may not be part of the vision, mission, or mandate of the host organizations in which these individual work but come together because of the importance of the problems at hand for example a crisis, environmental issues, human rights, conflicts, etc.). These temporary organizations can mobilize a great quantity of resources and synchronize activities very successfully as they are more focused on the problem than the maintenance over time of a permanent organizational structure.

At present, military organizations spend a major portion of their resources developing these coordinating capabilities. The present emphasis on Joint and Combined capabilities is long overdue, however, in wanting to achieve this coordination and synchronization, the present main focus of effort has been on trying to centralize control more than trying to put in place a new integration and coordination mechanisms. The present approach to Command and Control Information System interoperability through common standards indicates that the thought process and the push is still strictly aimed at a technology driven solution. As important that this is, there is still need for a command structure reengineering effort that permits faster decision cycles and a better integration of all the military information production elements such as Ops, Plans, Intelligence and Logistic Support. This coordination activity must includes central organizational elements such as Personnel, and Finance as well as the counterpart capabilities components of each of the Army, Navy and Air Force. The concomitant change that comes for accepting the Information Warfare framework is the requirement for a Command and Control Process Reengineering effort.

2.3 Virtual Information Environments

The military operating in an advanced computing environment would have the following essential elements:

- a. A hierarchy of powerful computing capabilities available to all personnel at all time, including portable computers, home computers, office computers, and various organizational and information production services. All stationary computers would be physically interconnected to very high bandwidth public networks. This means they are linked, for example, through fiber optic cables that allow large amounts of near real time multimedia information to be produced and distributed very quickly to selected consumers as well as being available on a pull basis to the rest of the community in case

the information is found relevant to other types of problems. Advances in remote telecommunications access technologies allow access to these resources without a permanent connection.

- b. Sophisticated interfaces that incorporate advanced cognitive ergonomic design concepts are employed. That is, the computers are extremely social. They have been designed to fit the way each individual works on a regular basis, even to fit the way people from different cultures work. The advances in Human Computer Interface have therefore enabled Social User Interfaces (SUI) that anticipates information requirements depending on the types of problems that is being worked on, the context and past requests. They support a variety on collection and communication, synthesis and visualization Knowbots. Knowbots and other software agents greatly simplify military personnel use of information technology. Knowbots are programs designed by their users to travel through a network, inspecting and understanding similar kinds of information, regardless of the language or form in which it is expressed. They produce the knowledge by linking of information. They act as templates that filter the information in accordance with prescribe rules and criteria. They are not just text retrieval processes but focus on concepts. Most of these Knowbots are active even when the user is not logged in.

2.4 Knowledge Based Work

Information is a strategic asset, however information is only one level of structure in an representational epistemological hierarchy. Information is organized data and data bases are prime repositories of data. They are structured in accordance with a ontological model called the data dictionary that enables a user to derive meaning from its contents. Not wanting to create an academic debate on the subject, suffice it to say that "knowledge is information organized for a particular purpose". [Nagao] It is the way information relates to other information that is of consequence to the discussion at hand. Furthermore, this knowledge may be returned into information databases becoming data for other information structuring processes. It is important to realize that Information Warfare is in part an issue of Knowledge Management. In itself information has no real value, it is the meta management issues that derive its worth to the problem at hand these meta- management issues can be regrouped under the heading of Knowledge Management.

2.4.1 From Information Management to Knowledge Management

As network technology matures differentiation and specialization of its components occur. Data-warehousing and massive archiving are now the problems of the day. Large organizations are starting to focus on the problems of storing and retrieving vast amounts of information. These massive data sets are being called different names such as Corporate Memories, Tactical Databases and Military Datasets. At the rate information is being produced and stored new data and information storage capabilities are now seen as the weak point in the modern networked information systems architecture. This problem encompass full life cycle issues such as the cost of capturing storing retrieving and distributing data and information.

Information manifests the "What is happening", knowledge personalizes "what does it mean" from the strict point of view of a single observer with his or her specific interests and needs. The

same information means different things to different people depending on the context. It is the creation of this context that is the central point of knowledge management. Knowledge Management addresses the problem of “relevance” or “pertinence” quality that information might or might not have with regard to other information. The same piece of information such as personnel status, depending on the context, could be of organizational, tactical, operational, or strategic importance. To make sense of vast amounts of information, to create the context by with this information becomes pertinent, that it means something to the user, it is necessary to use a schematization or a model that help highlight the nature of the relationships between this piece of information and another piece of information. These models, for example a series of tactical decision aids, also need to be managed as a unique critical component of the overall information system. Therefore there is now a clear requirement for Knowledge Management.

Knowledge Management presupposes that there is a sufficient level of modularity in the system so that data the models and schema (knowledge structuring processes) can be managed independently from the data. Data repositories would be separated from the query and search processes. It gives us the possibility to develop very sophisticated "intelligent assistants" such as an Anti Submarine Warfare Officer or a Navigation Officer. It must be understood that managing these models (expert paragon) would help truly confer to the system its effectiveness, whereas managing information confers only efficiencies.

Knowledge Management is still in its infancy refers to the problems associated with the creation, transformation, storage, usage, and replacement of highly complex models and computational structures that create meaning in an organizationally formalized way . Knowledge Management is arising as the focus of the next generation of software tools. At present this is yet to be fully structured but the figure illustrates the present supporting technologies.

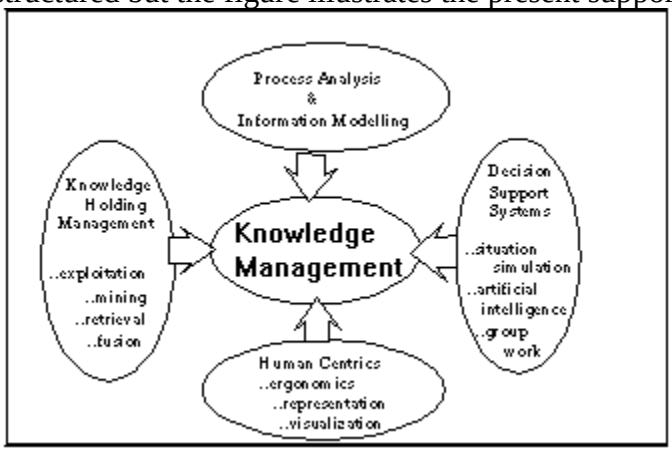

Figure 2
Knowledge Management Supporting Technologies

2.4.2 Knowledge Enabled Organizations

Having access to lots of information does not guarantee success. In all military estimates, the most important question is “What Does It Mean"?. The knowledge workers - the problem domain experts - are required to "make sense" of all that information. It is their insight into the

problems that will permit effective action. Knowledge is power only if it is acted upon. Domain specialists are the people in the field, but their capabilities are limited and their skills uneven.

Some people make good decisions are good while others are low on the learning curve. These decision making skills can be enhanced by systematic Knowledge Management. Three main functions need to be accomplished to enable any organization to pass from the level of simple artisans to having knowledge enabled workers as shown in figure 3. These are, Knowledge Formalization, Knowledge Abstraction and Knowledge Diffusion.

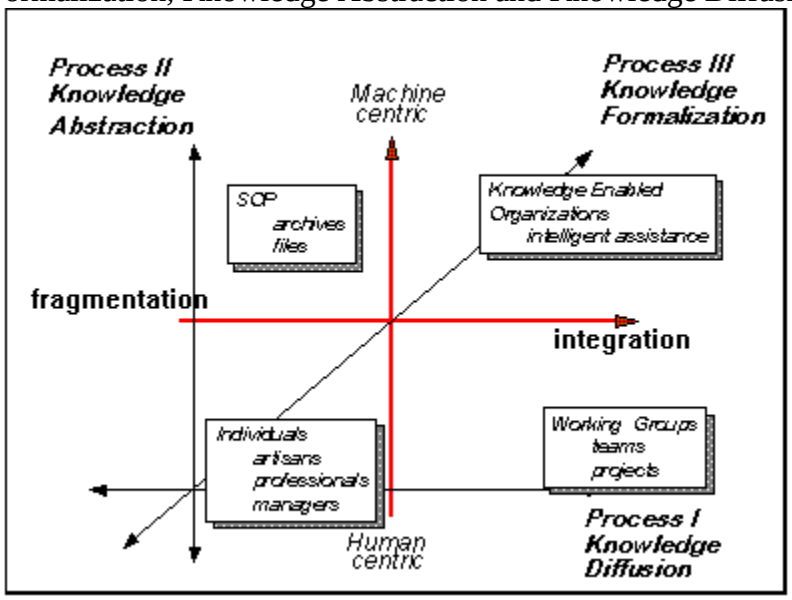

Figure 3
Knowledge Enable Organization

Capturing and replicating the best models and processes will help to increase the quality of the decision making processes. Case Base Reasoning Systems have proven invaluable in the area of Crisis Management. By capturing past cases and making them available to other users in support of decisions increases the number of options available to all decision makers and improves overall organizational performance. This even if the actual crisis has only some general similarities to past crises. This type of approach automates the "lessons learned" and makes them available to a user when similar conditions occur. Years of experience as well as the most recent policies and guidelines are made available based on the similarities between past cases and actual cases.

2.5 The IT Infrastructure - Global Networks

The origin of global networks can be debated. Some authors might say that it is international banking that was the first true global network. Some international companies have developed very extensive communication and transaction systems. World markets are seen as the reason for this globalization. However, in looking at the these examples of global networks they pale in comparison to the rise of the Internet. There is no system that reflects the democratization of information the way the Internet does. It is also known historically that communication

transforms humanity. The use of computers for international communication will further enhance and expand how humans connect, communicate and create communities. This bring with it new dimensions in world affairs.

2.5.1 The Origin of the Network

Some thirty years ago, the RAND Corporation, a think-tank, faced the question on how the US authorities would communicate after a nuclear war. How would the network itself be commanded and controlled as any central authority would be a target for an enemy missile.

The RAND proposal, made public in 1964, proposed a network with no central control and which would be designed to operate even with nodes destroyed. The proposal was to create a network built with unreliable elements but still could ensure that the total system would be reliable. All the nodes would communicate in a peer to peer fashion, each having the right to originate, pass, and receive messages. The messages themselves would be divided into packets and each packet would be separately addressed. Each packet would begin at some specified source node, and end at some other specified destination node without any requirement to specify the route to get there. Each packet would wind its way through the network on an individual basis with the total message being reconstructed at the end of the trip. If a node failed the packets would simply find another route to their destination. This structure became the foundation of the present system, Arpanet, which over time became the Internet.

2.5.2 Growth of the Internet

It is strange to say but nobody really knows the full extent of the Internet. There are estimates as to its size and growth. At present, April 1995, there are approximately 8 million host computers and between 10 and 50 million users connected to them. It's growth is truly an exponential curve. It's nodes doubled in the last year. According to the Massachusetts Institute of Technology, the total data that passed through the Internet Web service in 1992 was 500 MB. By comparison, the total data that was transmitted over the Web from January to March of 1993 was about 5 GB. The Total amount of data sent over the Web in a six hour period in September 1994 was 13 GB.

At present some say that the Internet population grows presently by 10 to 15 percent every month and doubles every 53 days; other say that by 2000 there will be as many as 100 million servers connect to the Net. The latest figures indicate that the Internet market (software,

hardware and services) is worth approximately $4.2 billion US.

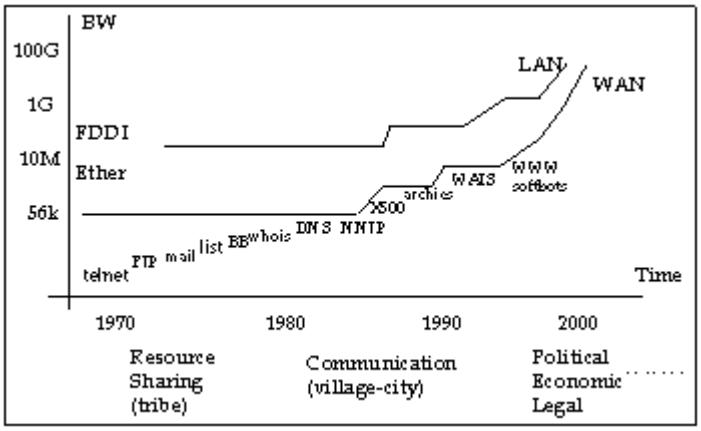

Figure 4
Growth of Global Networks

With the availability "Internet Ready" operating systems and free Internet browsing software, there is a situation that is so dynamic that predictions on the growth of the Internet and the resulting social effects are difficult to make. Furthermore, with new services such as video conferencing, digital cash, public key encryption, cybermalls, and virtual libraries being available throughout the system, there is difficulty in grasping fully the true extent of what an information based society is becoming. With simple access to global network organizations are shifting their focus away from the technology towards its social consequences. Its impact is now seen in the realignment of economic and social dynamics. All commercial organizations are forced to enter a truly global market place and with it the requirement to think and act both at a global level as well as a local level.

2.5.3 Interest Groups and Virtual Communities

There is a large discussion on the question of the true nature of communities that exists solely on the basis of the Internet. Non withstanding the debate, the ability to share common interests is sufficient for the Internet to bring together like minded individuals and organizations in such a fashion that forces us to review our concept of community.

The traditional interpretation of community includes a geographical aspect. But the Internet has no limitation that comes from geography nor national borders. A new type of communities are emerging that have the characteristic of being part of a global society - more accurate would be to talk about global societies. This further accelerated the growth of the Internet. At present no one would think of participating in any computer activity without being part of the Internet. Furthermore, not only for discussion of technical subjects these global societies, are also exemplified by a number of Non Governmental Organization (NGO) movements, interest groups, environmental organizations etc that find their leitmotif in social advocacy. In fact they are now a force in international relations, particularly with regard to crisis management, political concerns, and social issues such as human rights, and the environment simply because of their

internet enabled organization and structure. Finally the Internet itself is an proposal for universal value and an open society

2.5.4 Value Systems and Political Action

Discussion groups, or newsgroups, reflect focused discussions that occur within different communities. This is a world of news, debate and argument. It is generally known as the USENET. USENET is, in point of fact, quite different from the Web. USENET is rather like communities streams of consciousness reflecting on the subjects of the moment. USENET is not so much a physical network as a set of social meetings. At the moment there are some 3,500 separate newsgroups on USENET, and their discussions generate about 7 million words of typed commentary every day. Naturally there is a vast amount of talk about technology but the variety of subjects discussed is enormous and growing larger all the time. USENET also distributes various free scientific, social, and cultural electronic journals and publications.

As a consequence, global networks can enable the sharing of collective goals, aims and ideals, and permit the exchange relevant information amongst members. It also favors collective decision making by means of consensus and reciprocal relationships to meet the social, economic, cultural and world- wide problems of living in a what has become the Information Age. This positive scenario must be tempered with the fact that counter-forces will also come into play. A rise of organizations that favor dogmatism will also try to take advantage of global networks to further their specific aims and objectives. Already there are clear indications that tensions between opposing groups have resulted in benign forms of “netwar” such as the disrupting of phone, Fax and computer services. Furthermore they are passing from an individual to individual level to group to group level. This trend will continue with in some cases devastating consequences when some groups will use the power of the network to impose their control over other groups. They can use the network and its ability to leverage knowledge and power to restrict, control, manipulate and destroy other communities. Especially is these communities are dependent on the Internet as part of their infrastructure.

To balance out this perspective it is also important to acknowledge that the increased communication flows between individuals of differing communities, in addition to the official and sanctioned communication flows between governments, is seen as another way to reduce tensions between opposing groups. There is even a suggestion that putting in place rapidly an information infrastructure that is accessible by all, (not jut official or governmental decision makers) will reduce tension as more and more people communicate and resolve contentious issues1.

2.6 The Economics of Coordination and Cooperation

For many the sheer existence of the Internet is still a paradox. Why permit the give-away of so much information? It is seen as a gesture that would defeat the underlying competitive motivation that has been the motor of western civilization. Clearly the breaking down of organizational boundaries and the emergence of new types of loyalty and allegiances relationships between individuals and organizations introduces new modes of behavior. More and more individuals share their affiliation and loyalty between a number of organizations, some

of which have diverging agendas (for example we may all deal with environmental organizations, political parties, private corporations and government). However, in large economic markets an overall cooperative stance and strategy are more rational and leverage additional benefits than conflictual situation (as illustrated by recent game theory studies)2. Also, at the present, time there is very little cost in respect of the benefits of being part of a network such as the Internet.

Since each node is independent, handle its own financing and technical requirements, connecting to the Internet costs little or nothing if the organization you belong to is part of a network. Like the phone network, the computer network becomes steadily more valuable as it embraces larger and larger territories of people and resources. The more it grows the more it attracts and forces other users and networks to become part of it. The Internet was a novelty for a while, but networking is now an essential component of all social activities in all developed societies. Furthermore it is now a prerequisite to growth and development as well as maintenance of a quality of life.

2.6.1 The Creation of Wealth: Knowledge Versus Capital

Raw resources such as capital are becoming less and less a limiting factor in the production of goods and services as better processes improve our ability to substitute one component for another. Every day we witness whole sectors of the economy realign themselves to this constraint as automation leverages more and more economic output and displaces traditional production structures. We are now at a point where we can substitute information and knowledge for capital. The old adage "knowledge is power" is still true. Data, information or knowledge become readily available in a digital society. Open sources of intelligence as well as the emergence of the commercially driven Competitive Intelligence activities make data and information accessible to all. However it is the application of that information and knowledge that makes the real difference.

So it is not acquisition of knowledge for its own sake which is the goal, rather it is its innovative use that permits the creation of new capabilities. The military must understand that knowledge management is intended to support and spread innovation. What “one knows” rather than what “one owns” becomes the basis for social, political and economic action. And this power can be leveraged several times by embedding this information and knowledge into smart technology.

2.6.2 The Network as Broadcaster and Amplifier

One new dimension of technology and the network in particular is to act as a multiplier or an amplifier. As Electrical and mechanical systems amplify force, now network amplifies information. For the individual this means that in the network he can have the same capacity as larger organizations in the accomplishment of functions such as acquisition of information, distribution, storage etc. This can be done by an individual with using the network with a scope and expertise that rival what only governments and large corporations use to be able to do.

In many respects, this single capability to access and process vast amounts of information changes how public policy is developed. Access to statistical and demographic information has

always a factor in how public policy has been determined. But now this same capability is being used by individual, and organizations to challenge government.

2.7 Taxonomy and Natural Mutation of Information Systems

As information technology becomes more and more powerful, available and generic, the historical separation between organizational computer information systems and military computer information system will no longer be possible. The traditional classification of information systems based on specific intentions, and unique functionality can no more be applied. The traditional Automatic Data Processing (ADP) and Management Information Systems (MIS) on one hand, and operational and embedded mission systems on the other, will be subsumed an morphed into strategic information systems under the pressures and demands for information integration and system interoperability. Both outside and in DND there are important and powerful "tendances lourdes" - technical and functional trends that will condition and ultimately determine the nature of the evolution of our information systems. We will observe and experience several types of convergence:

2.7.1 Convergence of military and civilian systems

In a few years there will be little difference between information systems in the field and the ones in the office. Apart for differences in packaging, the hardware, the processor, and the communication interfaces will be similar if not the same. Systems can no longer be differentiated by hardware. Furthermore, most Office Automation (OA) software suites will be universal and will all have the same generic functions. The networks themselves, by virtue of their ability to interconnect will carry both organizational and operational information. In fact these networks will also support Other Government Departments (OGD) traffic.

2.7.2 Convergence of local and global scope.

Already there is a convergence towards unique military structure that will permit information to flow to and fro between the headquarters blending systems that had their initial purpose only by a geographical scope. As there will be in both cases to possibility to "see" the same data. The information systems will be both capable of global and local views. The possibility to "zoom in and out" or drilling into and out of areas of interest will continue to make the present notion of tactical and strategic systems somewhat ambiguous especially when coupled to remote sensors and effectors.

2.7.3 Convergence of functionality.

All environmental command and control information systems will have common subsystems, software applications and components. All will have a geographical information subsystem (GIS), message handling subsystem (MHS), Office Automation functions, voice and teleconferencing capabilities, etc. Here again there will be a requirement to rationalize their support at a national level. The timing requirements of real time vs. near real time will continue

to be the sole differentiating factor between strategic information systems and weapon systems. But real time and near real time data will be blended and fused so that organic information to the platform is fused with non organic information. Third party targeting and dynamic multi dimensional engagement based on force wide threat evaluation and weapon assignments will further force this trend.

2.7.4 Convergence of Representations.

With the emphasis on joint and combined operations there is a requirement for command and control systems to support a unified representation as well as the traditional environmental warfare views. There will be a requirement for common symbol sets and representations of all aspects of battlefield activities, as well as any conflictual situation such as peacekeeping and crisis management.

2.8 Tactical and Strategic Information Systems

The consequence of this "convergence" is that information can no longer be pre-defined in its nature as being solely strategic, tactical, operational or organizational. In the past the systems were clearly defined by the nature of their information content. The linking and networking of different information systems through the network abrogates the initial intention of these information systems, and now information that was once predetermined as being either organizational or operational are both simply managed as strategic. As information systems merge, information attribution is now more dependent on who and in what context it is used than where it is contained. Now it is better to focus on the decision making process as only will be able to assess the scope of consequence that will help qualify the military nature and context of the problem.

The discussion up to this point was to highlight and explain the unique initial conditions that have brought about the emergence of Information Warfare. The reason was to demonstrate the large number of qualitative discontinuities in the technical, social, and economic dimensions of information systems. Information Warfare is the result of these discontinuities. I would like to emphasize that Information Warfare is a new and unprecedented situation. Information Warfare is not a continuation of what was warfare. It is not just Command and Control Warfare nor is it Computer Warfare. These are manifestations of Information Warfare but as symptoms are not the consequence not the cause of a situation these initial denotations are simple and temporary interpretations of something much more complex, fundamental and revolutionary. Information Warfare is an emergent reality that comes from a self organization process that has never seen before. The problem is that we talk about it using terms that have well known connotations. And it is difficult to talk about something completely new using words that bring with them specific understanding and expectancies. The early period of the automobile faced a similar situation. At one time it was called a “horseless carriage” as this was the only way to define its essential quality. As the negation of the only understood means of propulsion - the horse. The car is more than a carriage without a horse. This is the dilemma we face when we discuss Information Warfare. Old words do not explain something new. and the danger is that the use of familiar words misrepresent and mask the true extend of the revolution that will have to take place if we are to be able to retain a military capacity in a new physical, social and cognitive space.

3. Information Warfare

There is a very extensive and broad discussion associated with the concept of Information Warfare and is difficult to distinguish true facts from pure speculation. However there is enough evidence to point to the reality of a new capability. Trying to define Information Warfare in a definitive way would lead to premature military policies as to what is and what is not Information Warfare. However, it is equally important to put forth some definitions that will help in bounding the problem and help in reviewing our traditional military warfare activities.

The various terms that are used in this area, Info-Doctrine, Cyberwar, Netwar and others terms indicate that it is still early in the debate. As yet nobody has put forth a set of definitive and complete tenets of Information Warfare. There are organizational effort to structure what are seen as Information Warfare activities. This permits a certain amount of classification work as to the threats, capabilities and objectives of Information Warfare. It is also evident, as presented earlier, that the emerging synergistic effects of Information Warfare require a more sophisticated conceptual framework so as to help integrate various the various traditional but separate capabilities such as EW, Intelligence collection, Target and Damage Assessment, IT security etc. The roles and mission of those capabilities are well known and need not be highlighted here. The intent here is to refine the understanding of Information Warfare by putting forth a conceptual framework and permits the development an action plan. Specifically towards the development of a military Information Warfare capability adapted to the requirements of an information based society.

3.1 Information Superiority

The guiding Vision for Information Warfare can be simply stated: Information Superiority through the availability and use of the right information, at the right place, at the right time, to all decision makers, while denying that information to the enemy. Information superiority is achieved through the development of Core Capabilities such as Knowledge Management, Joint Surveillance, Information Warfare and Information Technology. Information Warfare and Knowledge Management are new areas.

3.2 Definition of Information Warfare

There are several definitions of Information Warfare that are being put forward, mostly by US Military Organizations and Services. Whereas the Navy and Air force have Information Warfare capabilities, the Army is proposing Information Operations as being the mainstay of their conceptual approach. To be noted is that Russian Military Doctrine has always included the notion of Information Weapons; a fusion of advanced command and control, communications , intelligence systems, psychological and electronic warfare.

Information Warfare need to be seen as a cybernetic cycle. Observation, Analysis, Options Selection Decision Making, and Execution. This process is articulated in an Information Warfare Cycle as illustrated in figure 5.

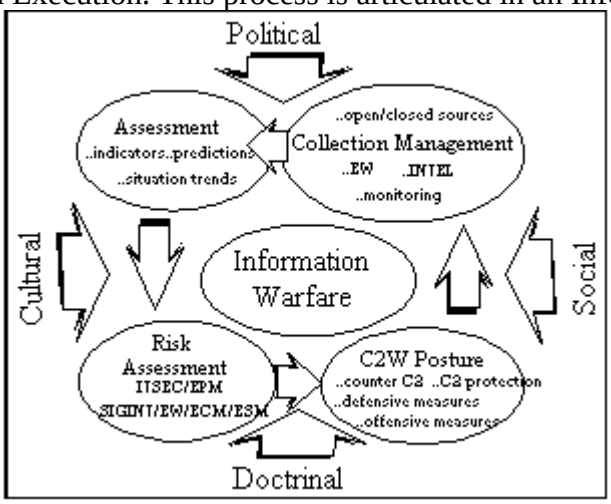

Figure 5
The Information Warfare Cycle

Information Warfare concerns itself with the control and manipulation of information and information flows. Specifically with the acquisition, process, storage, distribution and analysis of data and information. At a conceptual level, IW consists of all efforts to control, exploit, or deny an adversary's capability to collect, process, store, display, and distribute information, while at the same time preventing the enemy from doing the same. The intent is to control, manipulate, deny information, influence decisions, and degrade or ultimately destroy adversary systems while guarding friendly systems against such action.

This definition is quite broad but in many respects sufficient to show what Information Warfare as a concept authorize and legitimize new capabilities, as well as integrate the well established and understood arsenal of environmental capabilities (Joint, Army, Navy, Air Force) as well as concerned Governmental agencies.

3.3 Advantages of Information Warfare

As indicated earlier, it is in the new realm of networked systems that this definition finds its new applicability. To achieve information superiority in a networked information system prior to or in support of the traditional war fighting activities, offers the government and the military a whole new range of options never seen before:

- Information Warfare can prevent battle and reduce engagement. This will lead to more integrated and sophisticated conflict resolution activities prior to a military engagement.
- It will permit the maximum exploitation of all available and relevant information.
- It will help in exercising our understanding of the conflict in all its political, social, economic and cultural dimensions as well as facilitate action.
- It will ensure a superior use of our networks and Information Technology investments.

- It will create synergy by remove the logical and organizational barriers between the different units and capabilities. It will help focus Coordination and Cooperation at all stages of the conflict.
- It will facilitate change; and
- It will better explain past success and failures.

To support these objectives, new capabilities and skills are required. These expectations originate from the integration of the previously segregated activities such as Intelligence, Security, Joint and Combined Operations, Electronic Warfare, Psychological (Heart and Minds) type of Operations, supported by global and inter-operable Command and Control Information Systems.

3.4 Command and Control Warfare

We see that Information Warfare activities is not strictly done only by the military, it is an activity that need to be shouldered by a number of governmental agencies. No single service, agency or department is capable of doing all Information Warfare activities. It can only be achieved if the government brings all of its information production and exploitation assets to bear on a situation.

If Information Warfare is not just a military responsibility then there needs to a specific focal point for military Information Warfare activities. This area is called Command and Control Warfare. Without a doubt, however, the military bears the brunt for ensuring that IW activities are done such as peacekeeping and humanitarian aid. These are cases of concerted and coordinated efforts between Government agencies, NGO, and the military. But as always, in final analysis, it is the military that deploys or will be called to develop Information Warfare assets.

This proposes that in purely military terms, Command and Control Warfare capabilities will establish a large proportion of a government Information Warfare capability. Within military operations Joint Command and Control Warfare is the only appropriate avenue for Information Warfare activities directed against other Command and Control systems and requires that Joint Command and Control Information Systems become the military supporting infrastructure for conducting Information Warfare operations. Unfortunately this also begs the question if it appropriate for the military to support Information Warfare operations against other elements of a society's information infrastructure in periods that are not characterized by open warfare.

Command and Control Warfare focuses on trying to maintain control over enemy military Command and Control Information Systems assets. The problem is that Command and Control Warfare in itself lacks completeness since it does not integrate the broader strategic cultural, social, economic and political constraints into relevant action in support to the crisis management

activities that normally occur during the earlier phases of conflict as illustrated in figure 6.

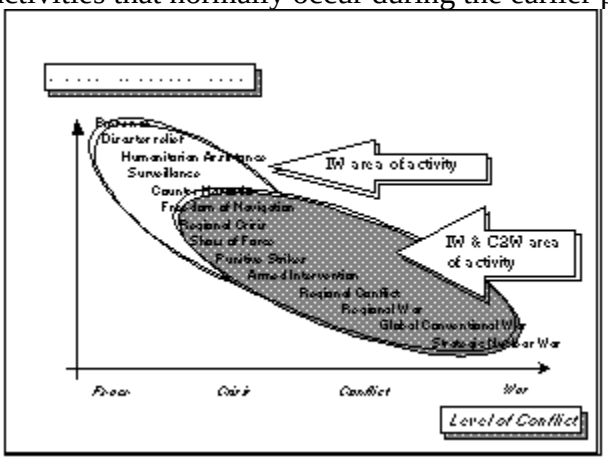

Figure 6
Spectrum of Military Activities

The US concept of Operation Other Than War (OOTW) is also address the fact that Information Warfare activities need to happen earlier in the spectrum of conflict activities than the ones purely associated with Command and Control Warfare activities. This therefore requires that the military and other agencies coordinate and cooperate in ways that have not been examined in the past. In Canada this is less of a problem because of our limited resources have always accentuated cooperation and coordination between Other Government Departments (OGD).

The recent development of a Canadian Maritime Network (CanMarNet) is an example of a interdepartmental information network that supports the exchange of maritime information between DND, the Department of Fisheries, the Coast Guard, and the RCMP. This system proved its value in the recent fishery conflict with Spain. And one can argue quite successfully that this conflict was a good example of Information Warfare. In this situation the military provided the surveillance, monitoring and communication infrastructure and the fisheries department acted in a lead capacity. These type of interdepartmental network will evolve and grow rapidly over the next few years. A governmental network will be able to mobilize and coordinate action throughout departments. Eventually, these networks will becomes elements of a larger government information infrastructure.

3.5 New Military Information System Vulnerabilities

At present Information Warfare in Canada is discussed more active in the private and civilian sector more than in the military. This because of US computer security organizations such as the National Computer Security Association (NCSA) that predict that an Information War will be waged against the most vulnerable elements and infrastructure components of a nation. And these are mostly civilian information infrastructure components. This is an easy target because an information intensive nation is very vulnerable to Information Warfare. Deliberate and planned computer sabotage, the seeding of viruses, global disinformation, and subversive control of a network could cripple the economy, wipe out banks savings, shut down phone systems, subvert trust and belief in democratic institutions and disrupt essential services and organizations.

Through data manipulation, theft, system sabotage and other means, entire economies and institutions may be rendered unworkable. These kinds of scenarios raise serious questions about who should have the capability to defend national interests. But it also blurs the distinction between military and civilian Information Warfare activities, mandates and responsibilities.

With the present military trend to acquire more and more commercial software and hardware products, and the growing need for system interoperability, for better or worse, the civilian information infrastructure, the governmental information infrastructure, and the military information infrastructure are going to amalgamate. This situation causes military infrastructure to be increasingly exposed. Furthermore these infrastructures are structurally weak and assailable because they are built using products that meet commercials needs first and not for military mission critical operations requirements.

Interoperability tends to stress standardization but too much computer system standardization is a liability and a destabilizing factor. Whole systems can become outdated or out performed by the creation of a new component. They can become incapacitated quickly, incapable of recovering from a single system wide attack on a single but common element to all components of the network such as a unique operating system or a unique communication protocol. A certain amount of controlled evolution through diversity confers to the network a certain amount of robustness and vitality.

3.6 Displacement of Warfighting Activities

Displacement in wealth producing activities have always from the less efficient sectors of activity towards efficient ones. As seen in the development of western society the creation of wealth has passed from agricultural sector, to industrialization sector, and is now centrally located in the information based activities. Each new structure of wealth creation subsumes previous or older ones. They do not totally replace them but incorporate them and make them more efficient. There is still an agricultural sector but it has gone through mechanization then industrialization and now digitization. More is produced with less people, resources and investment because the processes are so much more efficient. As societies fight the same way they create wealth then there will be also a displacement of focus of military capabilities. New way of warfigthing will never totally replace older capabilities but they will integrate them into more efficient processes as well as displace the focus of military activities towards newer and more effective configuration of technology and organizational structure.

Fighting conventional weapon systems requires well established military capabilities that rely on traditional hierarchical structure but faced with new vulnerabilities, a newer form of command structures with a more effective information infrastructure is required. It is within this newer command structure that the older military capabilities will be subsumed by the more effective command decision making processes. In this information age, we must know how to fight information wars as well as maintain our ability to fight the conventional wars.

3.7 Information Warfare Conceptual Framework

A conceptual framework must serve several purposes. It must be able to structure a series of new conceptual component by showing the causal relationships that exist between them. It must also be able to integrate older concepts into this explanatory scheme. This amalgam of old and new will help show what new capabilities and opportunities.

To fully analyze what Information Warfare bring to strategic analysis several new matrixes will be developed. The first one will be a Target Matrix. This will help in the classification problem of what is are different classes of target that Information Warfare focuses on. This second element of our conceptual framework is the Weapon Matrix. It will show the new arsenal that needed to wage a Information Warfare. Naturally most the discussion is about the potential of such "weapons" but as the capabilities exist today there is need to explore how they would be used during a conflict.

In order to build the most complete and congruent IW analytical framework possible, one that can apply in all situations using the Weapon and Target Matrix, a third one will be generated an Information Warfare Strategy and Planning Matrix based on possible targets and types of weapon needs to be developed. The strategic objective will determine both the type of target and the type of weapon. This matrix should be used as part of the strategic planning process. Along one axis Target Analysis will reveal the potential classes of targets. Along the second axis we can list the types of weapons that could be perpetrated against these targets. The resulting table offers insight as to the outcome of using a specific type of weapon on a specific target.

3.7.1 Information Warfare Target Analysis

The following Target Matrix is developed focused specifically on the decision making and its underlying support. If adversary decision making processes are paralyzed or subverted then the enemy system is under our control. This somewhat radical keeping in mind that several centuries of history have distilled principles of war but this approach is suitable to examine potential Information Warfare targets. There are presently other approaches that have their grounding in the capabilities themselves (Deception, EW, OPSEC, Psy Ops, Physical Destruction) but these are somewhat "bottom up" approaches. This framework is more abstract but somewhat more powerful than other proposals.

3.7.2 Types of Target

The aim is to attack or disable the principal or major decision makers via their information infrastructure. As seen in the earlier discussion on control , attacking the decision making mechanisms will directly affect the control of the system. The main targets classification method is around the binary relationship between goals and decision makers. Whatever the size of the adversary there is a fundamental relationship between the numbers of decision makers and the goals they seek to accomplish. There are three main categories: Single decision makers with single a single goal, multiple decision makers that share the same goal, and finally multiple decision makers with multiple goals (or not sharing the same one).

Any information systems can now be investigate in terms of a socio-technical structure. At present, the best way to go about it is to determine the decision nodes of the system. The could

be computer processes or users. By attacking these points the entire decision cycle as well the decision types (good or bad) and quality (timely, relevant, accurate) can be affected. It is necessary to discuss only categories of targets since this discussion is focused on the analytical framework.

3.7.2.1 Single Decision Maker /Single Goal

This is the monolithic organization. Mostly individuals or a very autocratic organization but could extend this class of targets to single central computational process (mainframe). Basically what we have here is a unique decision making process with a unique goal. It is a very focused target with a well bounded domain. All control functions are subject to this unique decision maker.

For example if we focus on attacking individuals we could either use their dependence on their system against them or focus the attack on their data shadow. Extensive reporting of privacy issues and problems have helped understand the problem. One could see how the information used in point of sale for purpose of restocking can be used to determine individual consumption habits that might interest insurance agencies for the determination of incidence of heart attacks and rate setting. Also in a rigid command and control organization focusing on the leaders severs the decision making capability from the rest of the organization making it somewhat headless. In the case of an unique computational process the whole system is brought down or subverted. This type of target is seen as relatively easy to attack and quite vulnerable. Modeling this class of targets is seen as quite feasible and of low difficulty.

3.7.2.2 Single Goal / Multiple Decision Makers

The next type of target is an control structure in which there are there are several points of control. They could be either automated or human and are distributed and could be dispersed over a geography but having the characteristic that all the decision making agents are focused on achieving a unique goal. This organizational structure is more complex but its dynamics are know and understood. Some archetype systems could be Command and Control Information Systems limited commercial and private business networks, .

This is the area of inter-organizational networks and governmental information infrastructure such as Saber and Wall Mart, America On Line, DREnet, etc. These systems are the pillars of a nation, its economy, and government services.

These structures have a major portion of their functionality that rely on sophisticated automated processes. Furthermore they are increasingly replacing human decision makers. Electronic Data Interchange (EDI), Financial Institution Message Authentication (FIMAS) and Just In Time logistic support are networks in which decision makers are primarily econometric models (as discussed in the Knowledge Management section). The shift from human to automated computer based decision makers is the trend in knowledge intensive organizations such as the military and specifically in command and control systems. Modeling these types of system are difficult and are principally based on stochastic/probabilistic, causal models, and time series extrapolation methods.

3.7.2.3 Multiple Goals / Multiple Decision Makers

In this class of targets we can group transnational and international organizations such as NATO, the United Nations, the European Union (EU), North American Free Trade Agreement (NAFTA) etc. Although these are emerging global structures, at the rate of network growth, these organizations will come to rely extensively on global information networks by the turn of the century. At this level it is possible that Information Warfare will take on the flavor of economic war. Continentalization of Europe, North America and the Pacific Rim nations postulates that tensions between and within this triumvirate will be forthcoming. It would be based on market capture and dwindling natural resources. In these ecological-like structures multiple decision makers are motivated according to specific but different agendas. Some of these objectives when taken as a whole might present several main poles of attractions. Polarization between these poles if they differ then conflict overtakes cooperation.

	Archetype Structure	***Reason for targeting Disruption of***	***Modeling Complexity***
Single DM/ Single Goal	Monolithic Hierarchy	Central control	Low (linear)
Multiple DM/ Single Goal	Organizations	Economy of scale Economy of force	medium (statistical)
Multiple DM/ Multiple Goals	National/ Transnational	Economy of scope Synergy	high (chaotic)

	Archetype Structure	Reason for targeting Disruption of	Modeling Complexity
Single DM/ Single Goal	Monolithic Hierarchy	Central control	Low (linear)
Multiple DM/ Single Goal	Organizations	Economy of scale Economy of force	medium (statistical)
Multiple DM/ Multiple Goals	National/ Transnational	Economy of scope Synergy	high (chaotic)

Table 1
Target Analysis Matrix

3.7.3 Types of Weapons

There has been a lot written recently on what would an Information Warfare look like. Scenarios focusing on Hacker Wars, Electronic Warfare, Information Blockades etc. have been developed. But here again these types of approaches are bottom up analysis that take their origin in specific capabilities. There has not been a systematic approach to an Information Warfare weapon taxonomy. At present time there are three main classes of weapons which could be used to wage Information Warfare. The classification is based on the effects of the weapons and not on the

weapons themselves. The effects of these Information Warfare Weapons can be Physical, Syntactical, or Semantic. The use of a physical weapon will result in the permanent destruction of physical components and denial of service. A Syntactical weapon will focus on attacking the operating logic of the system and introduce delays or unpredictable behaviors. A Semantical weapon will focus its effects on destroying the trust and truth maintenance components of the system.

As a general observation, the number of network attacks has increased tremendously over the last few years. This because it is not solely a technical problem. Tools of the hacking and cracking trade such as Satan, stealth and polymorphic virus builders are spurred on by the rapid spread of all kinds of public and private networks. Network analyzers and virus builder kits are readily available and at no costs. Knowledge and information about these tools and capabilities flows quite freely. So by leveraging both the power of these software tools and the weakness of a network, either surgical precision or massive disruption can be achieved on the overall decision making process of an organization.

Information Warfare weapon technology is not at present time a limiting factor but rather the present state of doctrinal, legal organizational knowledge about these issues. Couching the weapon capability in terms of Defensive versus Offensive Information Warfare is a discussion as to the legitimacy of Information Warfare activity. The US has approached this dilemma by separating Information Warfare into two distinct parts; Offensive Information Warfare (OIW) and Defensive Information Warfare (DIW).

The US military is focusing on developing a defensive capability only. This is seen as acceptable and a legitimate Information Warfare activity. But just doing DIW does not negate the necessity to probe and act in an aggressive way. These active capabilities are required in order to know to what extent are the vulnerabilities within their own systems. And to take these actions requires an active capability. An OIW capabilities. So talks about Defensive Information warfare without combining it with Offensive Information Warfare is missing out on the synergy that is required to become truly innovative in Information Warfare.

A Vulnerability Analysis capability is one of the means that ensure that an Information System has been efficiently and securely configured. Several essential activities must take place to perform Vulnerability Analysis such as probing to size the network and locate all its elements, determine access points, install agents and covert processes, explore, monitor and exploit. These are all “active” measures. For simulation and wargaming, Defensive Information Warfare needs an Offensive Information Warfare capability (Red cell) to achieve a relatively safe risk management stance. Turning the capabilities inward or outward, and calling them different things is a false separation as they are two sides of the same coin. But because of the sensitivities involved a Defensive Information Warfare stance is politically and legally a more acceptable position than Offensive Information Warfare. In order to develop a complete conceptual framework we must look at Information Warfare as a continuum going from a Defensive stance to an Offensive stance. As the DIW is a question of technical security and more a reaction to OIW, I will primarily focus on Offensive Information Warfare.

3.7.3.1 Physical Effects

This type of effect is achieved through weapon found in the realm of the traditional "hard steel on target". The physical destruction of any information structure offers complete denial of services. There are a number of capabilities that are available to do this and they comprises all the traditional weapon systems such as missiles, bombs, sabotage etc. Targeting for destruction a network is easy. A node and net evaluation must be done so as to cripple effectively the network. And this type of analysis applies to other supporting networks such as electrical and telephone grids etc.

Also there is more and more research being done on Directed Energy Weapons. They are categorized under the heading of Radio Frequency weapons. They are devices which destroy by radiating electromagnetic energy in the (RF) spectrum with wavelength's greater than 1 mm (frequency less than 3000 GHz). Suffice it to say that a pulse could have handicapped the operations at the World Trade Center more than the bomb did. These weapons are seen as a very important development because they enable non-lethal use of force. Technology demonstrators should be available within the next several years.

There is also the question that a system can be destroyed from the inside using malicious code, a virus. Virus can change setting that can permanently damage certain hardware components. But generally virus will destroy or corrupts data files and executable programs. As the denial of service would only be temporary. Recovery would be dependent on the availability of having planned disaster procedures such as having available CERT teams, mirrored and redundant systems using different hardware and software systems, or off site/off line data storage. So virus fall mainly within the next class of Information Warfare class of effects

3.7.3.2 Syntactic Effects

There new Information Warfare weapons have specifically emerge for the domain of information systems and networks. New viruses are being created an incredible rate as well as their counter-measures - anti viral software. Available now on the market are meta programming environments that "incubate" viruses in accordance with the desires of the attacker. The variety and combinations are daunting; Cruise viruses are capable of destroying specific data sets. Stealth virus conceal themselves from detectors and monitors. Polymorphic virus encrypt themselves using variable keys. There are also new Protected Mode viruses as well as the standard common file infector and boot sector viruses. This class of weapons aims to control or disable the operating logic of the targeted networks and systems. Using the operating systems software as well as the different utilities, the virus can make the system to act upon data in a different way or even simply waste cycles.

Virus need to be introduced into an information system either through infected discs or through a network connection. It is also to be noted that in most instance there is a separation between the data and the process that manipulates the data. But with the new Object Oriented Development (OOD) approach, data and process are packaged together. OOD supports modularity in system building and reuse of components. In many respects OOD is an ideal opportunity for planting and disseminating Trojan horses. All these issues are hotly debated and discussed. Technically the capability exist and he question for the military is what to do with such as capacity. Incidences of viral infection have risen but their spreading are less extensive due to the increased

use of anti-viral software. Incidents of system break-in have also risen in the last year. Cracker toolkits are so sophisticated that any weakness in a network will be found out quickly. New types of sophisticated network analyzers have several layers of heuristics built in. Cracking systems now has more to do with the sophistication of some of the Knowbots, tools and poor system security configuration (due to general lack of knowledge on the part of system administrators) than with the ingenuity of the perpetrators. Anomalies in systems behavior are normally not recorded if they occur in a purely random pattern. Virus that were meant to stay under "deep cover" could go undetected. For example some monitoring software application can check the clock, disable the modem speaker, place a call, transmit data and disconnect when done. There is a lot of fear that Internet software takes information off the user's disk and passes it over the network. Users are somewhat used to a bit of erratic behavior on the part of their system and would this would permit viruses to remain hidden for a long time if they act in an non disturbing way.

There is a discussion on what I call the Jeckel and Hyde virus that has its origin during the period in which memory was sparse and program had very little space in which to be stored. A program could be written so that it would run in a standard way but by bit shifting the code it could be run as a totally different program. The problem here is that this type of virus construction would be almost impossible to recognize as it is valid software in its first mode. Furthermore, virus that can make use of "cover channels and cover timing "3 capabilities to communicate would render even some aspect of security protection measures completely ineffective.

System vulnerabilities increasingly are being actively sought after and taken advantage of when found. Here lies one of the core doctrinal axiom of Information Warfare. Control the enemy's network and you control his decision making processes and his awareness and understanding of events. here is no requirement to destroy his systems or his data if this system is being controlled you. The use of Virus as Information Warfare weapon specifically targets the structural component of the information infrastructure i.e. the operating logic of the system.

3.7.3.3 Semantic Effects

The objective of this class of weapon is to affect and exploit the trust users have in the information system and the network, as well as affect their interpretation of the information it contains. Semantic Effects focus on manipulating modifying and destroying, the mental models, the awareness and representations that are developed, and constructed through the use of an information system. Whether it be a civilian organizational information system or a military command and control system. This is quite a challenge but this is the new dimensions of what use to be Psychological Operation, and Deception. These class of Information Warfare "weapons" alter the decision makers representation of what the information system portrays as the "real" world.

These weapons seek to affect not the information system itself but the behavior of the users and influence their decisions. The best way to think about these weapons are as "Memes" or virus of the minds that can be created via the information systems. Spoofing other peoples identity, selective spamming, broadcasting specific arguments and discourses, misinformation, slogans, and information overload can influence decision makers to a point where they misinterpret what

is happening. Humans have been employing this strategy for centuries in all but the case of networked systems this has taken a new dimension . Trying to recreate a close representation of what exactly is happening in the real world is the most difficult part of conflict management and warfare. However, this type of consideration will become more and more central to the Information Warfare debate as Social User Interfaces (SUI) start populating the systems. Interaction with Knowbots and Agents and other interface metaphors that might be subverted to show only specific types of data and information.

In the not so far future, multimedia information system environments will be the main information management tool. With this (still to be fully appreciated) context now needs to take into account the Freytag triangle4 of information attributes that show difficulty and requirement for more information rise and fall trough the specific phases of a crisis (exposition, inciting incident, rising action, climax, falling action and dénouement). As a consequence will require the user to rely even more on automated processes to search, retrieve, collate, and present information during the crucial information intensive phase of the crisis. The danger (or opportunity) is that the "dramatic orchestration" of what we believe as objective information is always grounded in a specific point of view and therefore open to manipulation.

Information always reflects something about its source and its purpose. Already in the inter-networked web where we can have both real-time and encyclopedic intelligence information fused from organic and non-organic sources computer mediated activities will enable the users to increase their active participation from the strict pragmatic response that come from the reading of a descriptive text narrative to a full emotional participation to a dramatic enactment of an event. This will change substantially the nature of operational activity as the immediacy and emotional closeness of the event circumvents much of the truth verification, the "sanity checks" processes that are usually constrained by longer decision cycles. The consequences of this "immediacy" of multimedia computer mediated interactions is a subject of research that is still in its infancy. The combination of highly emotionally charged pictures, sound, coupled to the personal engagement of the decision makers will open the avenue to vulnerabilities that come from intentional orchestration of preplanned discourse and events. Using morphed and altered images inserted during a live broadcast adversaries can use the response of such an orchestration to control rapidly and dramatically national decision making processes.

	Focus of the attack	***Primary Effect***	***Class of weapons***	***Modeli Comple.***
Physical	Physical	denial of service	hard steel	low (linear
Syntactical	Structural	operating logic obtrusion and corruption	virus, agents, filters.	mediu (statistic
Semantic	Behavioral	affecting users system trust and belief systems	Memes, dramatic orchestration	high (chaoti

Focus of the attack Primary Effect Class of weapons Modeling Complexit

Physical	Physical	denial of service	hard steel	y low (linear)
Syntactical	Structural	operating logic obtrusion and corruption	virus, agents, filters.	medium (statistical)
Semantic	Behavioral	affecting users system trust and belief systems	Memes, dramatic orchestration	high (chaotic)

Table 2
Information Warfare Weapon Matrix

3.8 Information Warfare Strategic Analysis Matrix (IWSM)

By placing the intended targets and the levels of effects in a table we create the final analysis matrix. The Information Warfare Strategic Analysis Matrix helps investigate meta- strategic issues that are derived from the planning and decision making process. The analysis centers around target selection, weapon selection and the analysis of the outcomes of such choices.

Information Warfare gives us a series of possible courses of actions, some of which are already well known and many new areas for which there are no capabilities yet. This final analysis matrix incorporates both past military capabilities and highlights areas in which Information Warfare activities demands the development of new offensive and defensive capabilities. It also drive us to seek a better understanding of what is truly Information Warfare.

In reviewing the IWSM we can deduce that the usage of well know capabilities such as hard steel has predictable outcomes. For example, if we wanted to physically destroy an individual's system, one could plant a virus that would destroy the data or some of the components making the system and the data unusable, blow up the system with a bomb, or even steal the system. Either way the results are the same. The effect is limited and controllable: denial of service. But this does not necessarily remove or eliminate the conflict. The intentionally is still there. Chances are that the conflict will find another outlet or tool set and continue anew. But this type of action has the advantage of imposing control and order so that other mechanism of conflict resolution such as political or governmental can be put in place to resolve or diffuse the conflict.

However the matrix point out that there are regions of unpredictable effects with unknown consequence in the management of the conflict. Further analysis is required in these areas, in order to develop an understanding, a capability and a defense. It is certain that Information Warfare activities will move toward these areas because they represent opportunities for high payoffs. They represent areas in which Information Superiority can be achieved without having recourse to the traditional military warfigting infrastructure. For very little costs a small organization can wage a pure information war without having to build an Army, Navy or Air Force. And it is specifically in these areas that our military must seek new understanding, capabilities and skills in order to recognize the treat and to defend ourselves against it.

3.8.1 Predictable Outcomes

In looking at the matrix we see that we already have capabilities to operate in some areas. Mostly these are areas in which any actions will produce predictable outcomes. These controllable outcomes can be generated by a host of actions. This includes the some elements of C2W such as EW and Physical Destruction. These effects are obtained through the usage of physical and syntactic class of weapon on single goal/single decision maker and single goal/multiple decision maker types of organizations.

For the military this encompass the traditional warfare area. It is possible to destroy physically all the information nodes of an dispersed organization but it is quite difficult. Suffice it to point out that such an objective could be achieved by a coordinated series of actions that destroy some of the more important elements of an information system this would achieve the same intended result. However, the propagation of a network virus may be much simpler and will have a much more damaging effect. In some circumstance simply delaying some computational processes may me sufficient to achieve the same goal. In a Just- In-Time army logistic system any delay caused by a purposefully planted syntactical level weapon will damage the effectiveness of any operation without the victim organization realizing it has being successfully defeated even before a physical engagement.

3.8.2 Unpredictable Outcomes

However, at present the use of Information Warfare weapons in other areas of the matrix will result in some unpredictable effects. In some cases in order to achieve information superiority, the creation of "ruptures" in the adversary's command and control systems as well as in the social, economic, and civil information infrastructure of the a country might be necessary. In well bounded and closed systems such as command and control information systems the effects of a syntactical weapon will have absolutely no collateral damage. But attacking some other systems will have as consequence a series of effects that will propagate through several other networks and have negative consequences on the final objective. Akin to shooting oneself in the foot.

	SDM/SG (Individual)	***MDM/SD (Organizational)***	***MDM/MG (Alliances))***
Hard steel	easy predictable	harder predictable	difficult predictable
Software Agents	harder predictable	***difficult unpredictable***	***very hard unpredictable***
Memes and Dramatic Orchestration	difficult predictable	***very hard unpredictable***	***very hard or very easy unpredictable***

```
                SDM/SG          MDM/SD          MDM/MG
              (Individual)   (Organizational  (Alliances))
                                    )
Hard steel        easy          harder          difficult
                predictable     predictable     predictable
```

Software Agents	harder predictable	difficult unpredictable	very hard unpredictable
Memes and Dramatic Orchestration	difficult predictable	very hard unpredictable	very hard or very easy unpredictable

Table 3
Information Warfare Strategic Analysis Matrix

Attacking an economic system will affect all economic system because they are all linked to one another in a global market place infrastructure. The reason for this comes from our understanding of nonlinear systems. Chaotic behavior in a system can explain some of these effects. Under certain initial conditions, some of the parameters can be made to create oscillation in the network, creating positive feedback in the control mechanisms. This results in catastrophic system behavior. This chaotic behavior is dependent on the linkages or "coupling" between the elements in the networks as well as in the linking relationship between the networks themselves. The system that will be targeted need to be investigated and the linkages need to be highlighted as to their sensitivity to propagate negative effects of Semantic Weapons. Systems and networks can either be loosely or tightly coupled.

3.8.2.1 Loosely Coupled Systems

Loosely coupled systems have a fair amount of buffering between the various common variables that are part of the different processes and elements. This buffering between systems permit more stable behavior overall . This stability is due to several underlying factors. Most of which are part of the information systems architecture involved. This applies to all three level of structures at the physical, syntactic and semantic level of the type of target structure. For example at the physical level of the Internet the architecture model allows for a fair number of failures and corruption and still remain survivable overall. But at the semantic level of the more active and radical Usernet groups the coupling is quite tight.

Information Systems that support distributed decision makers, must ensure a reasonable number of checks and balances and help maintain system stability. Disruption and full control of those systems is feasible but difficult because of the loosely coupled decision making processes. However as we automate and move up towards knowledge enabled organization then more and more computational processes will take over some of burden for routine decision making. This changes the interactions between organization from being loosely coupled to closely coupled.

3.8.2.2 Closely Coupled Systems

In closely coupled systems, then the prevailing conditions in one system can be amplified through the network to other systems. This can create the chaotic "butterfly effect" small local changes cause large effect because of positive nature of feedback and amplification in the network. Information systems, inter- networked organization, and even global networks, in times of crisis behave as tightly coupled systems. Positive feedback mechanisms will create severe ruptures in the normal order of system behavior, as seen in some of the stock market or engineering disasters 5.

Command and control information systems and their supporting networks are also closely coupled networks. Sensor to shooter coupling with distributed and network decision making will be subject to chaotic behavior especially if Rules of Engagement permit third party or remote firing. Recent failures of command and control systems in blue on blue engagements show how tightly coupled systems can fail. Taking advantages (control) of these closely coupling systems will be one of the challenge that Information Warfare presents to a modern military organization.

Waging Information Warfare using syntactic or semantic weapons will be particularly effective strategy if the target is a closely coupled network. Unfortunately the disruption will be such that the side effects could have a tremendous backlash within our own infrastructure. Inevitably, the effects will be transmitted to all participants in the network with unpredictable side effects and unforeseen disruptions. At present IW weapons do not have the capacity to limit such types of side effects, but it is this fact will not be lost on organizations that advocate terrorism as modus operande. These are well suited terrorist weapons. The development of Information Warfare defensive measures are essential as they will be necessary as part of a civil defense plan.

3.9 IW Control Models and Decision Systems

In developing this conceptual framework, several other concepts need to be touched upon. As Information Warfare is a new hypothesis of how traditional military activities position themselves in relation to one another. Our understanding of other concepts need to be reviewed and analyzed anew in context of this new representation of warfare. They are all elements of military capabilities such as the shifting role and loss of relative importance of the platforms in relation to the command and control network, the problem of control and decision making in a distributed organization, and the importance of developing a common shared representation of the conflict and the battlespace. These are all at present research domains but will become quickly central issues in the development of Information Warfare capabilities.

3.9.1 Sensors/Weapons and Platforms

There will be a fundamental shift in the relative importance of the role traditional platforms will have in the future. At present military organizations have a small number of large platforms all having a suitable mix of organic communication suites, dedicated and specific sensors slaved to a small number of unique weapons systems. Each have a command and control system but they are not well integrated as a whole except through limited bandwidth communication systems. In the future the emphasis will be to have a large numbers of much smaller platforms semi specialized around either sensors or weapons with a smaller command and control systems but all platform are very well integrated together through a unique and global command network.

The most important capability of this command network will be the ability to fuse organic and non-organic sensor information. No single platform will become the high value unit of the battleground. The allocation of targets to sensors to weapons will be done based on a dynamic assessment of critical priorities. Threat assessment and weapon assignment will no longer be at the platform level but at the force level. In this respect individual platforms will become secondary to the command and control infrastructure that will act as a super weapon/sensor system. Resource will shift from building the faster bullet to the more powerful algorithm.

3.9.2 From Simple Cybernetic to Multi-Agent Control

The growth of military command and control information networks will transform our idea of control. Traditionally, our military organizations have a rigid and hierarchical structure of decision making processes. The span of control should be congruent the scope and importance of the problem at hand problems. This also increases the confusion between what is tactical and strategic. A soldier in a foxhole is preoccupied with winning his battle, not the whole war, as there are too many elements outside his control but a decision at his level will in a way affect the course of the war. Was it a tactical situation or a strategic situation?

Our control exemplar is still based on the single decision maker cybernetic model of control faced with the problem of how to optimize a single goal under constraints of limited resources and time. This model served as a template for weapon systems design and has been adopted for most planning processes but it is of limited value when faced with the reality of several decision makers meshed in together through the use of command and control information system. The problem of predetermining the appropriate level of control to the right level becomes very difficult. If decision makers try to optimize the outcome at their level the result is a global sub-optimization. They win the battles but lose the war. This is the situation we face now. Because of the structure of military organization plays against the natural diffusion of control that comes from being a participant in a network. Network require different control structures than hierarchies.

One approach to this problem to try to enhance all the decision makers understanding of all the constraints faced by the group. If all the decision makers share the same common understanding of the battlefield they can in return adjust each their actions to maximize the outcome of all the decision take together. This approach is made possible through the use of information systems operating not a command and control systems but as cooperating, communicating, and coordinating system.

What emerges is a new mutation in the evolution of information systems. Computer Mediated cooperation systems that support the distribution and diffusion of control. This dissemination is function on how the decision makers concurrently and cooperatively build the context in which they will take decision. Each brings to the overall representation a fragment of information that can be used by others to better understand the overall context of their own actions and objectives. In Sum they are building a better global understanding of what is happening, see a better representation of what needs to be done and can they take decisions in concert with others to optimize all their resources for the problem at hand.

The essence of operational control would not be based on the focused understanding of single decision maker, but in a shared and common representation of the battleground in which each agent decides his own course of action based on his understanding of the total global picture. Much as a beehive behaves as a single entity even though it is composed of a multitude of independent actors. Coordination and synchronization mechanisms are not inherent to a hierarchical structure but from a peer to peer dialogue and mediation process based on consciousness and awareness mechanisms. This more complex model of control 6 however, will never replace at all levels the traditional military hierarchical structure. But it will certainly

displace some levels of command because it is a more flexible scheme that permits a faster adaptation of the organization to prevailing changes in the environment.

3.10 Visualization and Semiotics

Command and Control Information Systems continue to evolve. They will progress from being strictly closed military structures to open and interconnected true socio-technical structures. With a large number of participants in the network. Some of the participants have differing goals as well as in some cases different cultural background. This bring up the discussion of interpretation. and the requirement for the development of systems which fit different cognitive styles and have different presentation mechanisms. The use of military symbols is a case and point. For example, military tactical symbols and icons have unique importance in command and control systems. In many respects they have a unique grammar. They have a well defined set of formal rules for syntax, semantics, and pragmatics (reaction to a symbol that indicates an unknown). These military symbols will play a critical role in any future shared virtual environments. Until the system can represent, with a high degree of accuracy, the object itself, symbols will act as the main representation method. Symbols permit the rapid understanding of complex data and information, which range from physical attributes to final intentions. There are specific military symbols for almost all air, surface and subsurface objects. They can represent, foes, unknowns, jokers, prowlers etc. Military symbols associate by a single icon both the object and its intention. It is these representations that are the basis for all operational military situation assessment and decision making. In fact the present set of symbols are used as the basis for developing shared representation. Interoperability between military organizations is expressly based on the exchange of these symbol sets. However, semiotics analysis shows that the present military symbol set proposes only a limited and closed representation of a situation. In situations that do not require strict military action then these representation do not help in understanding what is happening.

Specifically, the present symbol set deals with only one phase of the conflict spectrum, the battle management phase. This is the last phase of an Information Warfare operation. It represents a defined problem area in that specific configurations of objects and events compose logical propositions that speak to, and about battle only. In future military Command and Control Information Systems, the present unique symbol sets, with their underlying phenomenology, create a frame of reference that both explains and predetermines a specific pragmatic response to these objects and events. This is the original intention of such a representation. These representations are very powerful and effective. But as military organizations are called upon more often to participate and act in earlier phases of conflict such as aid to civil defense, emergency response, humanitarian aid etc, as well as in Information Warfare activities then the present symbol set becomes a serious hindrance in both the understanding of the problem and the cooperative search for innovative solutions. A semiotically richer information environment is needed.

3.11 Officer Training and Education

The present capability of the Canadian Forces to select and prepare officers to operate under the constraint of the changing state of information technology falls short of the present and future needs of the Canadian Forces. The present selection and development process in the area of information systems is strictly a "reproduction" of passed officers experiences in strategic and tactical communications. It does not take into consideration the fundamental changes that have happened at the technical level as well as how information technology is changing the "Command and Control" field of study as well as their resulting concomitant impact on the CF structure and organization.

It is clear that in general the technical "revolution" and the new concepts of"Consultation, Command and Control" (C3) have not been integrated into the preparation of officers that will be responsible for these systems. The theoretical conceptual frameworks are absent in the areas of cognitive engineering, knowlegege engineering, and modern information system developement practices and methods. Only certain aspects of new information management techniques have been incorporated. Preparation for the problem of managing and fostering technical and scientific innovation is not part of the present curriculum.

Furthermore, and more seriously none of the aspects of how command and control information systems creates both order and disorder, and how it can be used to control uncertainty and instability are introduced any where in the educational process of an officer. These critical areas are not being presented or discussed. In fact the whole area of the impact of information systems on national security is not even mentioned. An awarness and an understanding of these issues and principles are fundamental in preparing individual that have the mandate to develop, field and operate information systems that will enable world wide action, national and international cooperation, and help in the management of incertitude as well as force and violence in support of conflict resolution.

4. Conclusion

It is acknowledged that Information Warfare is a reality that modern military organization will have to adapt to or be subject to it. New realities require new understandings and out of these understanding an evolution. New capabilities, organizations, skill sets as well as new modes of operation. For many this marks a turning point in military affairs as dramatic as when the airplane the tank or the radio became part of the military arsenal. But Information Warfare is even more dramatic than because it act in a systematic fashion in new dimensions. These are the abstract domains where knowledge created and information flows. Already we see that the open flows of information change the course of systems such as communism and other closed dogmatic systems. It is interesting to note that Information Warfare as a concept is in fact a meme that is growing in the mind of the common culture. If for nothing else we need to understand what it is so that we realize that there is no such thing as a silver bullet in warfare. Nor does any advantage stay for long on one side of the conflict. Information Warfare strictly as an element of an arsenal used to control will have its day shortly but more importantly Information Warfare also offers as a method a better understanding for the reasons of the conflict

in the first place. This in itself is more important. The discussion of what and how to use Information Warfare should be a discussion not just within the military or the government but in all areas of society. Information Warfare is all about meta strategy. A search and reflection on the causes and linkages of conflict.

In itself the research into a new concept requires the concomitant development of an epistemology, an ontology, and a methodology. I have presented elements of all three. But there is much more to do and to debate. This study of concepts was not intended to determine which capabilities should be developed nor how to integrate into present military operations Information Warfare nor to determine which units in our organizations will become keepers of this knowledge. This has yet to be done. But hopefully this report will help those mandated with such responsibilities to better understand why and what makes Information Warfare so different.

Information Warfare represent a new challenge for societies. As the tank and radio combined to change the concepts of maneuver so does the network and the virus. There is a need to continue to debate the issues raised in this analysis and to try to understand what the technology permits and what ethics and morality dictates. This is not the end of the debate on what is Information warfare - It is the start.

5. Bibliography

Advance Planning Briefing for Industry, "Winning the Information War", United States Army Communications- Electronics Command, Fort Monmouth, New Jersey. Symposium held May 11-12, 1994, Ocean Place Hilton Resort and Spa, Agenda and Description of Sessions, 10 pages.

Arquilla, John and Ronfeldt, David, "Cyberwar is Coming!", Article copyrighted 1993 by Taylor & Francis, Bristol, PA, originally published in the Journal Comparative Strategy, Volume 12, no. 2, pp. 141-165.

Benedickt, Michael Ed.. “Cyberspace - First steps”. MIT Press. Cambridge, 1991.

Burdea, Grigore and Coiffet, Phillipe. “Virtual Reality Technology” John Whiley and Sons Inc. New York. 1994.

Busey IV, Adm. James B., USN (Ret.), "Information Warfare Calculus Mandates Protective Actions", Presidents Commentary, Signal, October 1994, Official Publication of AFCEA, p.15.

Boyes, Jon. & Andriole, Stephen Ed. “Principles of Command and Control”. AFCEA International Press. Washington. DC. 1987

Campen, Alan D., ed., The First Information War, AFCEA International Press, Fairfax, VA, USA, October 1992.

Cook, Lt. Col. Wyatt C., "Information Warfare: A New Dimension in the Application of Air and Space Power", 1994 CJCS Strategy Essay Writing Contest Entry, Lt., 37 pages.

Collins H. “Artificial Expert - Social Knowledge and Intelligent Machines” MIT Press. 1990.

Defense Information Systems Agency, "Defensive Information Warfare (DIW)Management Plan", 15 August 1994, Version l.2, 4 sections and Appendices.

DeLanda, Manuel. "War in the age of Intelligent Machines", Zone Books Swerve edition New York 1991

Demchak, Chris. “military Organizations, Compleex Machines- Modernization in the US Armed Services”. Cornell University Press. 1991.

Dretske, Fred. “Knowledge and the Flow of Information”MIT press Cambridge Massachusets. 1981.

FitzGerald, Mary C., "Russian Views on Information Warfare", Army, Vol. 44, No. 5, May 1994, pp.57-60.

Franks, Frederick M.. Jr., "Winning the Information War: Evolution and Revolution", Speech delivered at the Association of the US Army Symposium, Orlando, Florida, February 8, 1994, Copyright City News Publishing Company Inc., 1994, 11 pages.

Garigue, Robert. "On Strategy, Decisions and the Evolution of Information Systems". Technical Document. DSIS DND Government of Canada. 1992

Garigue, Philippe. “Question de stratégie et de Métastratégie” Édition du GREF Collection Athéna Toronto 1992.

Heim, Michael. “The Metaphysics of Virtual Reality”. Oxford University Press. New York. 1993

Hurska, Jan. “Computer Viruses and Anti-Virus Warfare” Ellis Horwood Publishers. New York 1990.

Information Society Journal The, Volume 8, Number 1, 1992, Published Quarterly by Taylor & Francis, Printed by Burgess Science Press, Basingstoke, England.

Johnson, Craig L., "Information Warfare - Not a Paper War", Special Report, Journal of Electronic Defense, August '94, pp. 55- 58.

Johnson, Frederick C and Painter, Floyd C., "The Integration of Warfare Support Functions", Technology Analysis, Warfare Integration, C31:1988, pp. 176-182

Kelly AFB, Tex., "EW Expands Into Information Warfare", Electronic Warfare, Aviation Week & Space Technology/October 10, 1994, pp. 47-48.

Laurel, Brenda. “Computer as Theather” Addison-Wesley Publishing. Massachusetts. 1991.

Levy Pierre. “Les Techniques de l’intelligence - L’ avenir de la pensée a l’ère informatique”. Édition La Découverte, Paris 1990.

Levy Pierre. “La Machine univers - Création, cognition et culture informatique”. Édition La Découverte, Paris 1987.

Lum, Zachary A.,"Linking the Senses", Journal of Electronic Defense, August '94, pp. 33-38.

Luoma, William M., "Netwar: The Other Side of Information Warfare", 8 February 1994, A paper submitted to the Faculty of the Naval War College in partial satisfaction of the requirements of the Department of Joint Military Operations, 42 pages.

Nagao, Makoto. "Knowledge and Inference" Academic Press, Harcourt Brace Jovanvich, Publishers, Boston 1990.

Masuda, Yoneji. “The Information Society as Post Industrial Society”.Institute for the Infromation Society, Japan. 1981.

Poper, Karl. “The Logic Of Scientific Discovery”. Basic Books. New York. 1959.

Rosen, Stephen. “Winning the Next War - Innovation and the Moden Military” Cornell University Press. 1991.

Roos, John G., "Info Tech Info Power", Armed Forces Journal International, June 1994, pp. 31-36.

Science Application International Corporation (SAIC), "Planning Considerations for Defensive Information Warfare - Information Assurance -", 16 December 1993, 61 pages.

Sovereign, Michael G. and Sweet, Ricki Dr., "Evaluating Command and Control: A Modular Structure", Technology Analysis, Evaluating C2, C:31 1988, pp.-156-161.

Schwartau, Winn. "Information Warfare - Chaos on the electronic superhighway "Thunder's Mouth Press, New York . 1994

Toffler, Alvin & Heiddi. "War and Anti War" Boston: Little Brown, 1993.

Van Creveld, Martin. “Command In War” Harvard University Press. Cambridge. 1985

Ziman, John. “Reliable Knowledge - An Exploration of the Grounds for Befief in Science”. Cambridge University Press. Cambridge. 1978.

---

1 RAND Report

2 De Lamda

3 The Canadian Trusted Computer Product Evaluation Criteria Ver 3.0 Jan 1993

4 Breanda Laurel. Computers as Theater P.67

5 Foster Morrison The Art of Modeling Dynamic Systems-Forcasting for Chaos, Randoness, And Determinism. Mutiscience Press 1991

6 Pandamonium Model - De Landa - War in the Age of Intelligent Machines